

(54) FRAME SYNCHRONIZING CIRCUIT

(11) 63-220629 (A) (43) 13.9.1988 (19) JP

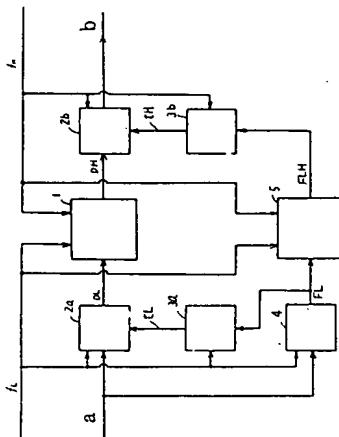
(21) Appl. No. 62-53819 (22) 9.3.1987

(71) FUJITSU LTD (72) TETSUO MORITAKA(1)

(51) Int. Cl. H04L7/08, H04J3/06

PURPOSE: To shorten a synchronizing recovery time by supplying the synchronizing information of input data before the speed is converted as it is, to a timing pulse generating device of an output side with one more elastic store in a synchronizing circuit using the elastic store.

CONSTITUTION: Synchronizing information FL of the low speed data before the speed conversion detected by an input side synchronizing detecting circuit 4 with a low speed clock fL is sent through an elastic store 5 to a high speed side timing pulse generating device 3b as it is. For this reason, even when a high speed side clock fH is temporarily turned off, the synchronizing information FL of input signal data is continued to be sent, and thus, when the high speed clock fH which is turned off is inputted again, the circuit can immediately enter the synchronizing condition.



a: input signal, b: output signal, fm: reading clock, 2a: input side data extracting pressing circuit, 2b: output side data extracting pressing circuit, 3a: input side timing generating device

(54) TERMINAL CONTROL SYSTEM

(11) 63-220630 (A) (43) 13.9.1988 (19) JP

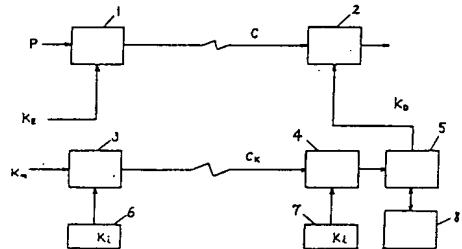
(21) Appl. No. 62-54559 (22) 10.3.1987

(71) MATSUSHITA ELECTRIC IND CO LTD (72) MASA YOSHI HIRASHIMA

(51) Int. Cl⁴. H04L9/02, G09C1/00

PURPOSE: To effectively prevent a wire tapping and to rapidly change the decoding program at a terminal by forming a decoding key with a program processing in a CATV system,etc., cyphering a program for forming a decoding key from a center, sending it to a terminal device and rewriting the above-mentioned program of the terminal device.

CONSTITUTION: At a center, an information signal P is cyphered by a cyphering key K_E and a cyphering information signal C is sent. At the terminal device side, the signal C is decoded by a decoding key K_D and an information signal P is reproduced. At a center side, a program K_n for making a decoding key K_C is cyphered by a key K_I from a key memory 6 and a cyphering key signal C_K is transmitted. At the terminal device, the signal C_K is received, the key K_I from a key memory 7 is used and the program K_n for making a decoding key is reproduced by a decoding part 4. After the K_n is received and stored into a memory 8 by a decoding key making part 5, the decoding key K_D is made and supplied to a decoding part 2 with a program for making a decoding key including K_n . Consequently, regularly or irregularly, the encoding key K_E is changed at a center side.



1.3: cyphering part

(54) MESSAGE TRANSFER SYSTEM

(11) 63-220631 (A) (43) 13.9.1988 (19) JP

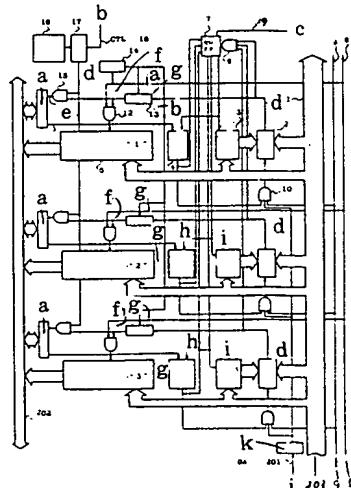
(21) Appl. No. 62-53808 (22) 9.3.1987

(71) HITACHI LTD (72) YASUHIRO TAKAHASHI(1)

(51) Int. Cl. H04L11/00

PURPOSE: To maintain the number of buffers of a node to the necessary minimum by providing a means to register an opponent address which is a receiving object, a means to recognize a transmitting source address and a means to discriminate a receiving/non-receiving action in a receiving circuit.

CONSTITUTION: A comparator 2 compares a transmitting source address SA of the received packet and the contents of an address register 3, and at the time of the transmitting source for a first time, an empty message buffer 5 is selected by a selector 7, the SA is registered to the register 3, a flag register 4 for empty closed displaying is set and the data are fetched into the buffer 5. For the succeeding packet from the same node, only the data part is fetched into the same buffer. For the packet of other node, when the buffer exists in which the address is coincident, receiving is executed to it, and when the above-mentioned buffer does not exist and the buffer, in which the register 4 shows emptiness, exists, it is registered to the register 3 and the data are fetched. Except the above-mentioned case, loop answer (LA) information is returned to a sender. Thus, with the message restoring completion as a unit, the buffer is shared and thus, the capacity can be decreased.



16: end packet pattern, b: to CTL analyzing 109, d: coincident, c: to LA pattern generation 110, e: buffer l message completion, f: permission, g: reset, h: set, i: setting, k: delaying, j: from comparing 107, 203: receiving data bus, 9: SA timing, 8: data timing, l: read completion instruction, 10: LA information, 13: latch, 14: delay, 18: CLT information, a: register

⑩ 日本国特許庁 (JP)

⑪ 特許出願公開

⑫ 公開特許公報 (A)

昭63-220630

⑬ Int.Cl.⁴

H 04 L 9/02
G 09 C 1/00

識別記号

府内整理番号

Z-7240-5K
7368-5B

⑭ 公開 昭和63年(1988)9月13日

審査請求 未請求 発明の数 1 (全6頁)

⑮ 発明の名称 端末制御方式

⑯ 特 願 昭62-54559

⑰ 出 願 昭62(1987)3月10日

⑱ 発明者 平嶋 正芳 大阪府門真市大字門真1006番地 松下電器産業株式会社内
⑲ 出願人 松下電器産業株式会社 大阪府門真市大字門真1006番地
⑳ 代理人 弁理士 中尾 敏男 外1名

明細書

1、発明の名称

端末制御方式

2、特許請求の範囲

(1) センターから情報信号を暗号化して送出し、この暗号化された情報信号を端末機で所定の復合化鍵で復号化する端末制御方式であって、前記端末機において前記復号化鍵を形成する機能の少くとも一部をマイクロコンピューター等の演算手段によるプログラム処理により行なうようになり、前記センターから前記復号化鍵形成用のプログラムの少くとも一部を暗号化してプログラム情報として前記端末機に送出し、このプログラム情報をより前記端末機の前記プログラムを書き換えるようにしたことを特徴とする端末制御方式。

(2) 複数個の端末機毎に群とし、各端末機群毎に暗号化プログラム情報の暗号化及び復号化の鍵の組合せを変更するようにした事を特徴とする特許請求の範囲第1項記載の端末制御方式。

3、発明の詳細を説明

産業上の利用分野

本発明は、CATVシステムやDBSシステム等の有料放送における暗号化情報信号の送受信を行う場合などに用いることのできる端末制御方式に関する。

従来の技術

有料放送システムにおいて情報を暗号化して伝送し、受信側(端末側)で復号化して受信する一般的な例について、第4図を参照しながら説明する(例えば、一松信監修「データ保護と暗号化の研究」第6章図1-27)。第4図に示す。

この方式はMIX方式と呼ばれ、送信側で情報信号Pを暗号化部201で鍵K₁により暗号化して伝送する。また、公開されているRSA方式の暗号化鍵K₂を用いて鍵K₂を暗号化部203で暗号化し、暗号化された鍵C₂を端末機側へ伝送する。端末機側では、RSA方式の復号化鍵K₃を用いて復号化部204で鍵C₂を復号してDES方式の鍵K₁を得る。送信側では鍵K₁を用いてDES方

式により情報信号Pを暗号化部201で暗号化し、暗号化信号Cを伝送する。端末機側では、既に得ている鍵K_iを用いて暗号化信号Cを復号化部202で復号化し、情報信号Pを得る。

発明が解決しようとする問題点

この方式を一方向アドレッサブルCATV放送或は衛星放送に適用した場合を考えると、暗号化鍵K_iと復号化鍵K_nの組合せが端末の数だけ必要となり、しかも盗聴を防ぐために桁数を多くすると鍵K_iを全端末へ配達するためのアクセスするのに長時間を必要とするという問題がある。鍵K_iとK_nを秘密の鍵としてもアクセス時間は同じだけ必要となる。

又、全端末共通の鍵K_i, K_nとすれば1台で盗聴された時に全端末で盗聴されるという影響が生じ、或はK_iを固定にしても1台で盗聴されれば全端末で盗聴される。

本発明は、かかる従来の欠点を解消して、暗号化された鍵の解説による盗聴を有効に防止することができる、しかも、多くの端末に対してその復号

化プログラムを短時間に変更することのできる端末制御方式を提供することを目的とする。

問題点を解決するための手段

上記問題点を解決するために、本発明の端末制御方式においては、センターから情報信号を暗号化して送出し、この暗号化された情報信号を端末機で所定の復号化鍵で復号化する端末制御方式において、端末機において復号化鍵を形成する機能の少くとも一部をマイクロコンピューター等の演算手段によるプログラム処理により行なうようにし、センターから復号化鍵形成用のプログラムの少くとも一部を暗号化してプログラム情報として端末機に送出し、このプログラム情報により端末機の前記プログラムを替えるようにしたことを特徴とする。

作用

かかる構成によれば、センターから端末機側へ伝送する復号化鍵形成用のプログラム内容を定期的にあるいは不定期に変更して端末機の復号化鍵形成用プログラムを変更することができ、不法に

解説されて盗聴されても直ちにその盗聴を不可能にすることができる、暗号化情報の盗聴を有効に防止することができる。

実施例

以下、本発明の一実施例について、図面を参照して説明する。

まず、第1図に本発明を実施する一例のシステム構成を示す。

センターにおいては、情報信号Pを暗号化部1により暗号化鍵K_iによって暗号化し、暗号化情報信号Cを送出する。端末機側では、この暗号化情報信号Cを受信し、復号化部2で復号化鍵K_nを用いて復号化して情報信号Pを再生する。

センター側では、さらに、復号化鍵K_n作成用のプログラムK_nを暗号化部3で鍵メモリ6からの鍵K_iにより暗号化して、暗号化鍵信号C_xを伝送する。このプログラムK_nは、端末機で使用する復号化鍵作成用プログラムの全部であっても、その一部であってもよい。この暗号化鍵信号C_xは、暗号化情報信号Cの垂直プランギング期間等に

挿入して伝送すればよい。

一方、端末機では、この暗号化鍵信号C_xを受信し、まず、鍵メモリ7からの鍵K_iを用いて復号化部4で復号化鍵作成用のプログラムK_nを再生する。この鍵K_iは、ROMやICカードの形等で端末機に具備される。次に、復号化鍵作成部6でこのプログラムK_nを受け取り、メモリ8に格納した後、その伝送されてきたプログラムK_nを含む復号化鍵作成用プログラムを用いて復号化鍵K_nを作成して、情報信号復号用の復号化部2に供給する。

従って、この構成によれば、定期的にあるいは盗聴のおそれが発見された時等に、センター側で情報信号暗号化用の暗号化鍵K_iを変更し、それに伴ってその復号用の復号化鍵K_nを作成するためのプログラムK_nをも変更して伝送することにより、それまでに可能になっていたかもしれない盗聴行為を全く無効にすることができます、不法な盗聴を有効に防止することができる。

第2図に、メモリ8を他の処理プログラム用と

ア ページ

兼用したときのアドレスマップの一例を示す。ここには、復号化部4で鍵 K_1 を用いて暗号化鍵信号 C_k を復号化するプログラム①およびその他の情報信号復号化用等のスクリンブル処理プログラム、ここでは述べていないが課金処理を行うための課金プログラム、および復号化鍵作成用プログラム等が格納されており、EPROM等で構成されている。本システムでは、このうちの復号化鍵作成用プログラムの全部又は一部をセンター側からの暗号化鍵信号 C_k を用いて書き換え変更する。

次に、端末機における信号処理回路の具体例を第3図に示す。この例では、暗号化情報信号 D の解説処理も暗号化鍵信号 C_k の解説処理も同一のマイクロプロセッサを用いて行なう。まず、伝送されてきた暗号化鍵信号 C_k を入出力レジスタ11で受け取り、その旨をマイクロプロセッサ(CPU)12に伝達する。CPU12は、ROMで構成した鍵メモリ A_M から予め端末機毎にセットされている鍵 K_1 を読み出し、PN発生回路13をこの鍵 K_1 に従って制御して所定の復号化用PN信号

を発生する。この復号化用PN信号により、ZX-OR回路14で上記の暗号化鍵信号 C_k を解説して復号化鍵作成用プログラムを再生し、EEPROMで構成したプログラム用メモリ B_M に書き込む。このプログラム用メモリ B_M の内容は、次に新たに暗号化鍵信号 C_k が伝送されてきて書き換えられるまで保持される。上述した如く、この暗号化鍵信号 C_k によって書き換えるプログラム K_n は、復号化鍵作成用プログラムの全部であっても、その一部であってもよい。

次に、CPU12はプログラム用メモリ B_M から復号化鍵作成用プログラムを読み出し、それに従ってPN発生回路16を制御して、所定の復号化鍵 K_n を作成する。

そこで、暗号化情報信号 D が伝送されてきて入出力レジスタ11に入力されたときに、この復号化鍵 K_n を用いて復号化部2のZX-OR回路16でその暗号化情報信号を解説し、CPU12の制御により入出力レジスタ11から復号化した情報信号 P を出力することにより、情報信号を受信す

シ ページ

10

ることができる。

なお、17はCPU12のワークRAMである。この構成によれば、鍵メモリ A_M の鍵 K_1 とプログラム用メモリ B_M の復号化鍵作成用プログラムとが描い、かつCPU12、PN発生回路13、15による処理動作が所定のものとなったときにのみ、暗号化情報信号 D を復号して再生受信することができるるので、盗聴に対してきわめて強いシステムを構成することができる。

また、第3図における入出力レジスタ11、CPU12、および各メモリ A_M 、 B_M 、17を1チップ化してICで構成することにより第三者による解析を困難にすることができる。さらに、PN発生回路13、15およびZX-OR回路14、16等の復号化部分も同時に一枚の基板上に実装しつつモールドしたりパッケージングすることにより、ハイブリッドIC化することができてさらに盗聴のための解析等を防止することができる。

さらに、上記実施例以外にも、各復号化部および復号化鍵作成部等をハードロジック回路で構成

したり、CPUを用いたソフト処理回路で構成したり、それらの混合により構成することができる。たとえば、PN発生回路13、15は、ハードロジック回路でも、ソフト処理でも容易に実施できる。

次に、本発明を用いた場合の復号化鍵作成用プログラムの伝送時間について、従来方式と比較して説明する。

まず、端末数を3000万台としデータ伝送レートを現在衛星テレビジョン放送(BS)で使用されている音声チャンネルを利用して暗号化鍵信号を伝送するものとしてその伝送レートと同一の240Kbpsとし、データパケットをBest方式によるデータ190ビット、訂正ビット82ビットおよびヘッダ16ビットの合計288ビット構成とする。

従来の第4図の方式の場合は、各端末における復号化処理プログラムが同であるので、盗聴を有效地に防止するためには各端末毎に暗号化鍵信号 C_k を伝送する必要がある。この暗号化鍵信号 C_k を

D E S 暗号化方式で伝送すると 64 ビットが必要となり、これに 3000 万台の各端末を識別するためのアドレスが最低 25 ビット ($2^{25} > 3000$ 万) 必要になって、合計 89 ビットで 1 端末分の暗号化鍵信号 C_k を伝送することができる。従って、1 パケット (288 ビット) 当り 2 端末分の C_k を伝送することができる。故に、1 秒当たりの伝送可能端末数は

$$\frac{24(\text{Kbps})}{288(\text{ビット})} \times 2 = 1666.7(\text{台/秒})$$

となり、3000 万台の端末に 1 通り C_k を伝送するためには、

$$\frac{3000(\text{万台})}{1666.7(\text{台/秒})} = 1800\text{秒} = 5(\text{時間})$$

を要する。

一方、本発明の方式において、1 パケット中の 160 ビットを用いて暗号化鍵信号 C_k を伝送することとし、50 パケット分で 8000 ビットすなわち 1 K バイトの 1 つの暗号化鍵信号 C_k を伝送することとする。さらに、本方式では復号化鍵作

成用のプログラムを変更するものであることから全端末毎に全て異ならせる必要はない。そこで、この暗号化鍵信号 C_k の種類を 1 万種類とすると、1 通り C_k を伝送するためには、

$$\frac{24(\text{Kbps})}{288(\text{ビット}) \times 50(\text{パケット})} = 16.67(\text{台/秒})$$

$$\frac{3000(\text{万台})}{16.67(\text{台/秒}) \times 1(\text{万種類})} = 180\text{秒} = 3\text{分}$$

で伝送することができる。

発明の効果

以上のように、本発明によれば、情報信号を暗号化して伝送するとともに、その復号化のために必要な復号化鍵作成用プログラムを伝送して端末機の復号化処理用プログラムを書き換えるようしているので、このプログラムを定期的に、あるいは監聽のおそれがあるときにセンター側で変更することにより、監聽を有效地に防止することができるものである。

4. 図面の簡単な説明

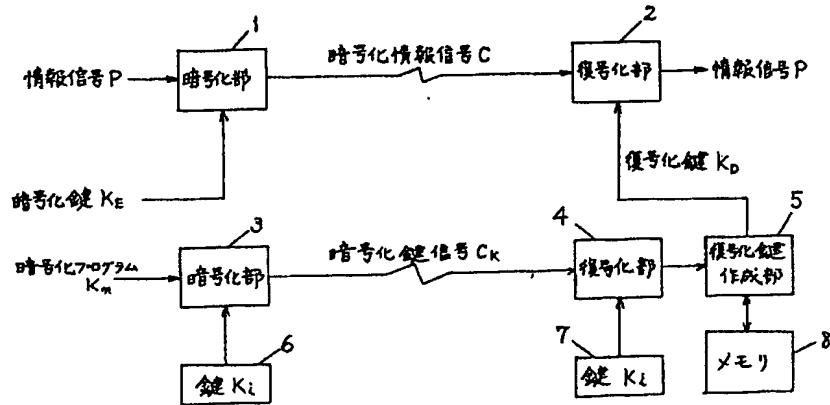
第 1 図は本発明の端末制御方式を実施した一例

のシステムのブロック図、第 2 図はそのメモリのアドレスマップ図、第 3 図はその要部の具体ブロック図、第 4 図は従来方式を実施した一例のシステムのブロック図である。

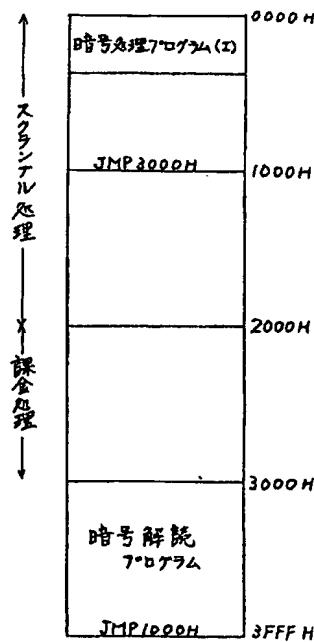
1 ……暗号化部、2 ……復号化部、3 ……暗号化部、4 ……復号化部、5 ……復号化鍵作成部、6 ……鍵、7 ……鍵、8 ……メモリ。

代理人の氏名 弁理士 中 尾 敏 男 ほか 1 名

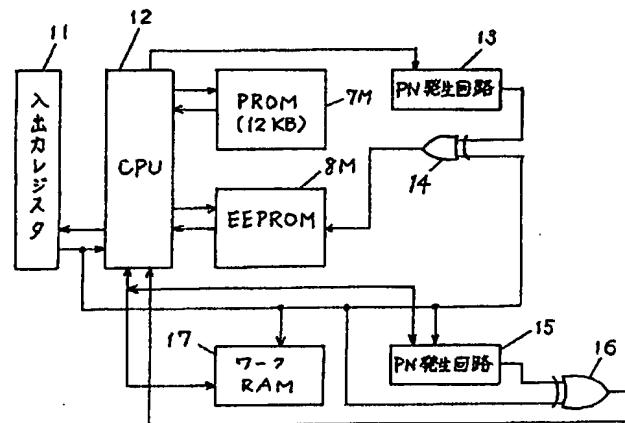
第 1 圖



第 2 図



第3図



第4図

